PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	Michael Freed; Elango Ganesan	Confirmation No.	4136
Serial No.:	09/900,494		
Filed:	July 6, 2001	Customer No.:	28863
Examiner:	Aravind K. Moorthy		
Group Art Unit:	2131		
Docket No.:	1014-064US01/JNP-0261		
Title:	LOAD BALANCING SECURE SOCKETS LAYER ACCELERATOR		

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicants respectfully request a Pre-Appeal Brief Request for Review. Details of some the Examiner's errors are set forth below. For simplicity and brevity, Applicants have focused the arguments below on pending independent claim 1 to demonstrate the Examiner's error. By setting forth the clear grounds of error, Applicants do not assert that these are the only errors that the Examiner has made, nor do Applicants waive any arguments that may be asserted in an Appeal Brief.

Rejection under 35 U.S.C. 112, first paragraph

In the Final Office Action, the Examiner rejected claim 1 under 35 U.S.C. 112, first paragraph, asserting that the specification fails to describe the claimed subject matter in such a way to enable one skilled in the art to make and/use the invention. In the Advisory Action the Examiner stated that, with respect to claim 1, he could not find support in the specification that the "decryption engine and the load balancing engine bypass an application layer of a network stack by decrypting the data from the secure communication sessions of the clients and

outputting the decrypted data to the associated server devices without processing the data with the application layer of the network stack."

Applicants' previous responses directed the Examiner's attention to Fig. 3 and the related description that describe an SSL accelerator that does not process secure SSL data received from the web client at the application layer (e.g., HTTP) prior to forwarding the packets to the web server. Instead, the SSL accelerator shown in Figure 3 intercepts data destined for the web server and, rather than the transmitting packets up and down the TCP/IP stack as shown in Figure 2B, will perform the SSL encryption and decryption below the application layer and at the packet level before forwarding the packet on to its destination.[1]

In the Advisory Action, the Examiner stated that he had reviewed Fig. 3 and only found the description related to the SSL accelerator. Thus, it appears that the Examiner recognizes that Applicants' SSL device decrypts data from a secure communication sessions of the clients and outputting the decrypted data to the associated server devices without processing the data with the application layer of the network stack, as required by claim 1. However, the Examiner appears to question whether the specification provides support for a load balancing engine that bypasses the application layer of the network stack, as also required by claim 1. On this point, pg. 10, ll. 14-18 of the present application specifically states that the SSL accelerator of FIG. 3 supports a number of different operational modes of encryption and decryption, including a "load-balancing mode." In this manner, when performing SSL and performing encryption or decryption at the packet layer by bypassing the application layer (as discussed in detail with respect to FIG. 3), the SSL accelerator can specifically operate in a "load-balancing mode," which is discussed in detail in FIG. 6.

One of ordinary skill would appreciate that the claim limitation of a decryption engine and a load balancing engine that bypass an application layer of a network stack by decrypting the data from the secure communication sessions of the clients and outputting the decrypted data to the associated server devices without processing the data with the application layer of the network stack, as recited in claim 1, correctly represents the operation of embodiments of Applicants' acceleration device enabled within the present application. Applicants' specification

[1] Specification, pg. 10, ll. 8–12.

describes the claimed subject matter in such a way to enable one skilled in the art to make and/use the invention. The rejection under 35 USC 112, first paragraph, should be withdrawn

Rejection of claim 1 under § 103

In the Final Office Action, the Examiner rejected claim 1 under 35 U.S.C. 103(a) as being unpatentable over Hankinson et al. (USPN 6,799,202) ("Hankinson") in view of Toporek et al. (USPN 6,654,344) ("Toporek").

In the Advisory Action, the Examiner states that Hankinson discloses an encryption/decryption engine in a TCP/IP and SSL environment.[2] The Examiner correctly recognizes that Hankinson describes conventional support for SSL, i.e., where application data is reassembled via the application layer for decryption well above the network layer and physical layer.

To address this deficiency of Hankinson, the Examiner relies on Toporek because "it allows the network layer to communicate directly to the physical layer."[3] On this basis, the Examiner rejects Applicants' claim 1 under 35 USC § 103 over Hankison in view of Toporek. Therefore, the Examiner's case for obviousness is founded on Hankinson (which teaches that SSL encryption and decryption is implemented conventionally at the application layer) in view of Toporek that teaches a satellite gateway that relays information directly between the network layer and the physical layer without processing the relayed information.

The Examiner's reasoning is based entirely on the unsupported assumption that the Toporek process for relaying information could be applied to decrypting SSL secure client communications of Hankinson. Applicants are left to wonder how in the world one of ordinary skill could implement an SSL acceleration device and load balancer that operates at the packet level and bypasses the application layer, as claimed by the Applicants, based on (1) a reference that teaches conventional SSL at the application layer, in view of (2) a reference that teaches relaying information between the network layer and the physical layer without processing the information. The Examiner assumes that somehow these references could be combined so that

[2] Hankinson at Summary.
[3] Office Action, pg. 5, where the Examiner cites Toporek at col. 11, ll. 22–33.

one of ordinary skill would be able to implement SSL and load balancing without processing the SSL records at an application layer.

SSL records are generated at the application layer. Decrypting SSL records without processing the SSL records at the application layer is a non-trivial problem for which a solution is provided in Applicants' specification. Such a technique is not remotely answered or suggested by any of the references, even when viewed in combination. Even when viewing the references in combination, there is a significant gap in the teachings of the cited references as to how such a feature may even be implemented. The fact that Hankinson describes conventional SSL and that Toporek describes a mechanism for simply relaying packet information without processing the packets at all provides no teaching as to how encrypted communications could be decrypted with an acceleration device without processing the secure data at the application layer. Even when viewed in combination, Hankinson and Toporek provide no solution as to how to load balance and decrypt an SSL or other secure communication session with an intermediate device without processing the secure data at the application layer.

The Examiner's only response to this point in the Advisory Action was to state that Applicants' arguments attach the references individually. This is an inaccurate characterization of the facts. Applicants' argument is that the Hankinson in view of Toporek, even when viewed in combination, provide no teaching as to how load balancing and decryption of secure communications could possibly be performed in the Hankinson device without processing the secure data at the application layer. Hankinson's conventional SSL approach in view of Toporek satellite gateway that merely relays information without processing the information provides no teaching whatsoever that would allow one of ordinary skill in the art to implement such a feature. Hankinson's conventional approach certainly could not be used below the application layer, and Hankinson in view of Toporek provides no other teachings whatsoever that would solve the complex issue of how SSL records could be decrypted and load balanced without processing the SSL records at the application layer.

For at least the reasons set forth above, Applicants request a review and a panel decision that promptly resolves the issues and eliminates the need for an Appellate Brief at this time. Please charge any additional fees or credit any overpayment to deposit account number 50-1778.

Date: August 21, 2006

By: Kent J. Sieffert

SHUMAKER & SIEFFERT, P.A.
8425 Seasons Parkway, Suite 105
St. Paul, Minnesota 55125

Name: Kent J. Sieffert
Reg. No.: 41,312